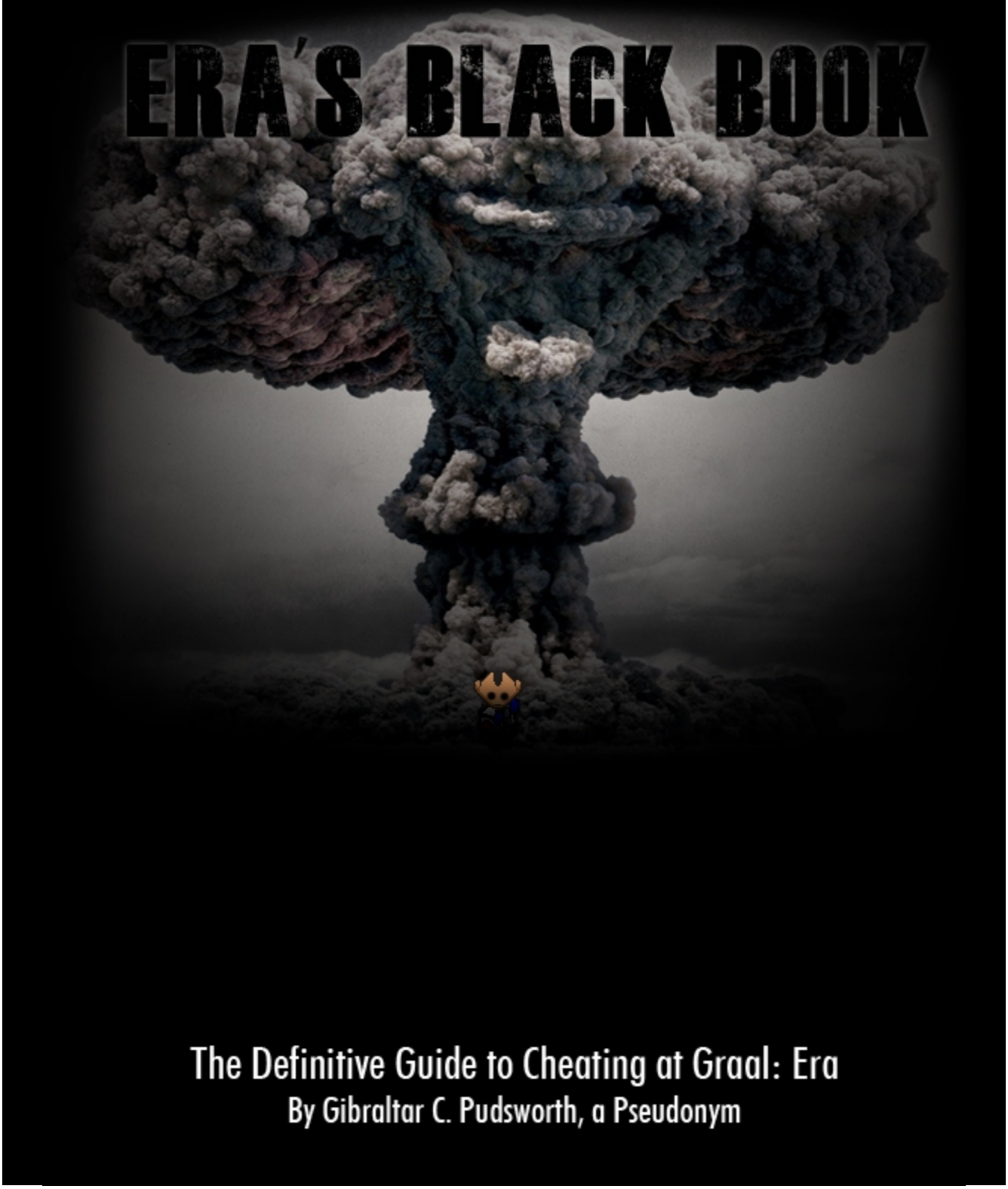
ERA'S BLACK BOOK



The Definitive Guide to Cheating at Graal: Era

By Gibraltar C. Pudsworth, a Pseudonym

Table of Contents

-Introduction.....3
-Bots.....4
-Lag Switches.....7
-Laming.....11
-Combat Assistant Scripts.....12
-Taunts and Random Chat.....14
-Disguises, Deception, And Dirty Fucking Lies.....15
-Client Modification.....17
-Extra Accounts.....18
-Covering Your Tracks.....19
-Farming Mystery Coins.....19
-Running Multiple Clients.....20
-Running Blacklisted Applications.....20
-Using Blacklisted Applications.....21
-Using Graal Relay.....22
-Gani Hacks.....24
-In-Game Exploits.....24
-Account Theft.....25
-Other Attack Vectors.....27
-Case Files.....28
-Conclusion.....31
-Credits.....31

Introduction

I've been cheating on Era for a long time. Over the years, I've gotten better and learned many tricks along the way. I'm such a cheating bastard, in fact, that I find more entertainment value in breaking the rules and playing Era the wrong way. Let's face it – Era is a poorly managed mess of a game. Once you learn how the system works, it's fairly easy to slip through the cracks. ~~I've managed to avoid discovery (and subsequent punishment) of my cheating. My luck might run out some day, however, which is why I've written this document.~~ If I'm ever threatened with a ban, my plan is to use this guide as an insurance policy – to wave it in the face of whatever admin catches me, and to make threats of my own. Namely, to release this document to Era's unwashed denizens - to teach them to cheat, and in doing so, compromise the whole server's balance. In that sense, this guide is designed to be Era's weapon of mass destruction – a collection of dangerous knowledge which, together, has the power to undermine Era's economy and teach everybody how to break the rules and collectively ruin the game. If you are an average player, I suggest that you start using these methods. With the release of this document, you are now at a disadvantage if you're playing fairly.

Figure A: FUCK DA POLICE

~~Or maybe I've decided to quit on my own, and I've released this file for shits and giggles. Even better, maybe I personally sent you a copy, and I want you to be my cheating buddy.~~[1] However you obtained a copy, I urge you to use, and abuse, these methods to their fullest extent. Then find even better ones.

Break the game, because that's way more fun than actually playing it.

1 Global ban. I was found botting and was offered a warning if I confessed. This offer was immediately rescinded once I confessed, and Era's staff were not receptive to my threats, hence the release of this document.

Bots

Most online games force their players to perform mindless, repetitive tasks for hours in order to earn fictional currencies in order to buy shinier weaponry. That's boring. Bots can be scripted to perform these repetitive tasks for their human masters, so we'll have time to go outside and talk to girls (or maybe not). GlovePIE is one of my favorite programs for this sort of thing. It's primarily intended as a scriptable language for remapping the function of various input devices, in order to make PC gaming a bit easier. I use it to script bots. [http://glovepie.org/glovepie.php] The software's author has seen fit to include some strange anti-Israel licensing conditions and random bullshit about global warming, but if you ignore that quirk, it's a useful application. An example of use is press A, wait a tenth of a second, release A, and repeat. Pair this with walking instructions, and a bot can be made to execute the same movements over and over again, which works fairly well in a consistent context. I often use a pizza-bot at Speedy Pizza. Since it's an indoor area, it's secluded, and therefore low-profile. It's also a no-pk zone, so people won't kill my bots. In GlovePIE, I made this bot for automated pizza-making:

```
/*
  Pizza macro. Equip pizza peel and face fourth from left pizza table
  (second column, second row)
  Can make roughly $9 per 12 seconds, or about $45/min.
*/

 var.wait_time = 110
if pressed (console) or var.runloop = 1 {
var.runloop = 0
//Start make dough
   wait 2s
wait 50ms
press (a)
wait var.wait_time ms
release (a)
wait 400ms
//End Make Dough
//Start Get Sauce
press (right)
wait 10ms
press (up)
wait 175ms
release (up)
wait 300ms
release (right)
wait var.wait_time ms
press (right)
wait var.wait_time ms
release (right)
wait var.wait_time ms
press (a)
wait var.wait_time ms
release (a)
wait var.wait_time ms
wait 750ms
//End Get Sauce
//Start Walk to pizza
/*
press (left)
wait 350ms
release (left)
wait var.wait_time ms
press (down)
wait 300ms
release (down)
*/
press (left)
wait 10ms
press (down)
wait 215ms
release (down)
release (left)
wait var.wait_time ms
/*
press (right)
wait 65ms
release (right)
wait 50ms
*/
```

```
press (down)
wait 50ms
release (down)
wait 50ms
press (a)
wait var.wait_time ms
release (a)
wait 250ms
//End Walk to Pizza

//Start Get cheese
press (right)
wait 475ms
release (right)
wait var.wait_time ms
press (up)
wait 280ms
release (up)
wait var.wait_time ms
press (right)
wait var.wait_time ms
release (right)
wait var.wait_time ms
press (a)
wait var.wait_time ms
release (a)
wait var.wait_time ms
wait 900ms
//End Get cheese
//Start Walk to pizza
press (left)
wait 250ms
release (left)
wait var.wait_time ms
press (down)
wait 450ms
release (down)
wait var.wait_time ms
/*
press (right)
wait 65ms
release (right)
wait 50ms
press (down)
wait 50ms
release (down)
wait 50ms
*/
press (a)
wait 100ms
release (a)
wait 230ms
//End Walk to Pizza
//Start Get pepperoni
press (right)
wait 475ms
release (right)
wait var.wait_time ms
press (a)
wait var.wait_time ms
release (a)
wait var.wait_time ms
wait 800ms
/*
press (up)
wait 200ms
release (up)
wait var.wait_time ms
//End Get pepperoni
//Start Walk to pizza

press (left)
wait 350ms
release (left)
wait var.wait_time ms
press (down)
wait 250ms
release (down)
wait var.wait_time ms
press (right)
wait 65ms
release (right)
wait 50ms
*/
press (left)
wait 200ms
release (left)
wait 50ms
press (down)
wait 50ms
release (down)
wait 50ms
press (a)
wait var.wait_time ms
release (a)
wait 230ms
//End Walk to Pizza
```

```
//Start Walk to pizza
press (left)
wait 350ms
release (left)
wait var.wait_time ms
press (down)
wait 380ms
release (down)
wait var.wait_time ms
press (a)
wait var.wait_time ms
release (a)
wait 230ms
//End Walk to Pizza
*/

//put in oven
/*
press (right)
wait 65ms
release (right)
wait 50ms
*/
press (down)
wait 50ms
release (down)
wait 50ms
press (d)
wait 250ms
release (d)
wait var.wait_time ms
press (up)
wait 1000ms
release (up)
wait var.wait_time ms
press (d)
wait var.wait_time ms
release (d)
wait 400ms
/*
press (left)
wait 40ms
release (left)
wait 10ms
*/
press (down)
wait 800ms
release (down)
wait var.wait_time ms

*/
wait 100ms
var.runloop = 1

}

if pressed (end) {
say ("Stopping macro")
exitprogram
}
                                                                    //End
```

It works fairly well. Pizza-making is a relatively low-end job on Era, but it's simple enough for a bot to do. You still need to babysit the bot, as sudden lag-spikes can cause it become misaligned in its motions, requiring the user to reset it. Also, admins or savvy users might recognize it as a bot. I've done work to counteract these problems. In fact, the above example is quite outdated. I've come to transition to using GlovePIE as more of a rapid-prototyping tool for bots, to figure out the timing. Once finalized, I port it over to a stand-alone executable program using AutoIt. This results in a much more flexible program. Executable files also run more quickly than GlovePIE scripts, which seems to result in a smoother bot which is less likely to malfunction. One of the biggest upgrades is the ability to send key presses to the Era window, even when it's minimized, allowing me to surf the internet and whatnot as it runs in the background.

I plan on adding features such as random human-like movements (to seem less robotic) and a means of detecting misalignment using image detection, or by reading the color of a specific pixel (as, at a certain point in the pizza cycle, pixel X should be color Y. If not, the bot will reset its position). Such features could allow a bot to work for you all day while you go snort cocaine off of a mummified koala-penis or something. I have many other bots, with varying degrees of success, for various tasks. I have included a companion file full of source code (because look at that mess up there. I don't want all

of that clutter...). I've made bots for mining, digging shells, stocking in businesses (you just jam A. So simple...), idling to avoid a disconnect, making coffee, and lumberjacking.

Some bots aren't strictly for making money. Other tasks are just as boring. My prime example is Era's gym. You can lift weights to carry more shit, but why bother? It takes forever. I initially tried to make a bot for this using GlovePIE, but the timing in the weight-lifting minigame is randomly generated, so I couldn't make a bot which could predict the timing with any accuracy. After a good bit of research online, I found that the aforementioned AutoIt can perform image-recognition with the Image Search library. You simply take a screenshot, crop it to show the visual cue (in this case, the word “Lift!”), and make your AutoIt application press A when it sees that image on your screen. This bot works *incredibly well*, not only working faster and more efficiently than a human player, but very reliably as well. This method is a great way to tip the scales in your favor (literally, I guess. Shitty weight pun), because you'll be able to haul tons of different weapons around, or carry more rocks, trash, shells, or wood when you're working. The source code is included in the companion file.

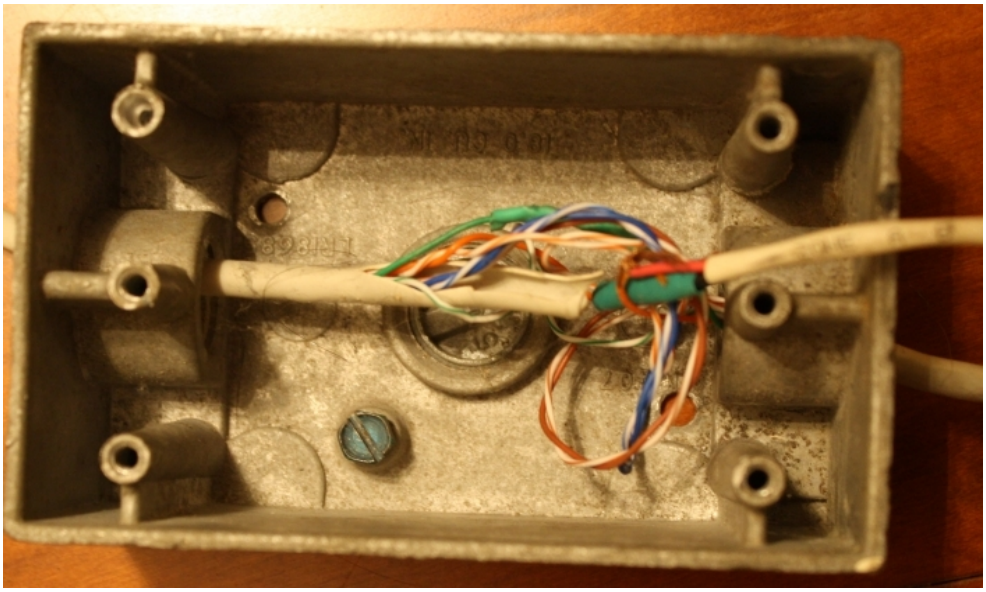
This concept – the ability to give your bots graphical input – opens the door to many other cool possibilities. For example, I made a mining bot *which can actually detect the presence of other players*. This is useful for maintaining stealth, and allowing you to relax and trust that your bot can function relatively unattended. To check for players, I simply held down the period key in a macro and hovered the mouse over a GUI element which lists players on a map. If a pixel on the second slot is white, then that indicates the presence of another player (possibly an admin or a snitch). When a player is detected, my bot ceases its activity and presses CTRL+B to flash the “BRB” bubble. Essentially, I have programmed my bot to whistle innocently when people get too close. This bot is able to level up quickly, because it works tirelessly and more efficiently than any human could. Thus, it will actually become more efficient and more profitable as time goes on. I believe that this makes it extraordinarily threatening to Era's economy. Source code will be included with this release.

Lag Switches

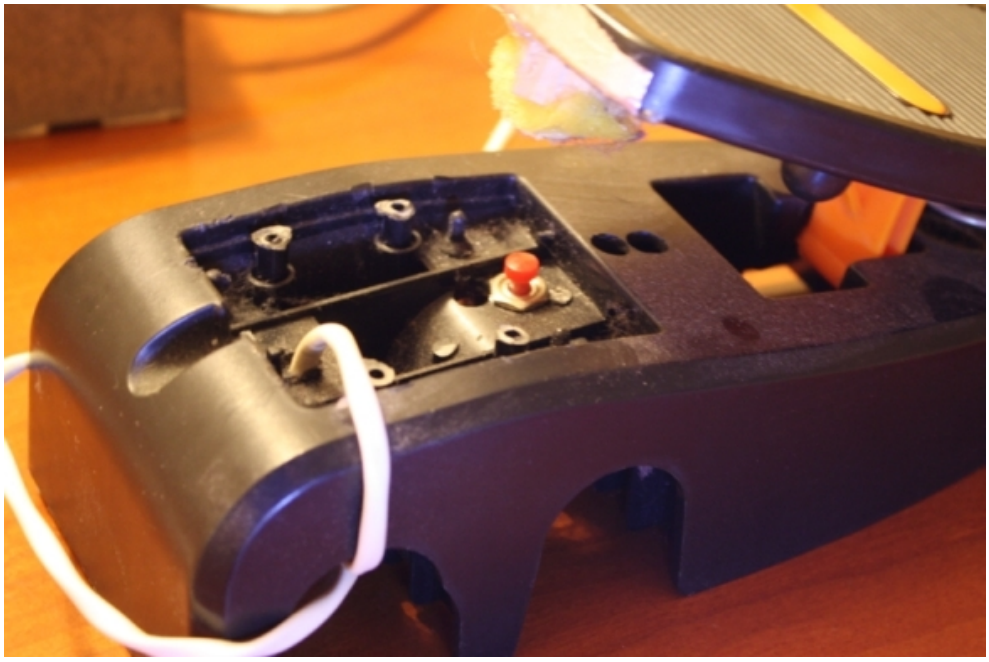
This one is just wonderful. Anybody can download a trainer off the internet, but building a physical device with which to cheat is so much more rewarding. A lag switch is a physical device which temporarily interrupts a network connection at your command. To make one, simply cut open a CAT5 cable (noob translation: INTERNET PIPE), and cut a wire (I've found that orange and green work well, but your color coding may vary), and install a switch. This is the most basic way to do it, but if you'd like to get fancy, as I have, you can build it into a project enclosure and wire up a foot pedal to activate it. My build details are as such:

I took an old Rock Band foot-pedal (which I scored for free from a friend) and gutted out the old electronics. I bought a normally-closed momentary push button from Radio Shack (it's a few bucks for, like, four of them). The “normally-closed” part is important. Most switches are “normally-open”, meaning that the electrical circuit is not completed. When you press a normally-closed button, it breaks the connection, which you'll need for a lag switch. Otherwise, your internet connection will just be fucked up. Forever. Anyhow, I took the foot pedal to the ol' drill press and put a hole in the plastic frame under the foot-piece, and installed the button there so that it would be pressed when the pedal is down. Some hot-glue and soldering makes it sturdy enough to sit under a desk. Hook it up to your snipped CAT5 cable and you're ready to go. Keep in mind, a foot pedal isn't required – I just decided to make mine a bit easier to use in the heat of battle. Any old toggle-switch will work.

Foot Pedal Lag-switch



Wiring box – notice that the orange wire is spliced into a separate cable, which leads out to the foot-pedal. I have since added a panel to cover this mess. I don't advise that you let it all hang out like this.



Foot-pedal, and the Normally-closed push button.

You just hook up the lag switch in between your computer and your internet connection. If you're using Wifi, put the switch between your router and its hardwired cable. Once everything is hooked up correctly, jump into Era and disconnect for a few seconds. This will sever the connection between your client and the server. As far as the server is concerned, you haven't moved. It thinks you're just lagging. However, once you re-establish the connection, you will suddenly fly to whatever position your client is at. You will appear to teleport around your opponents, giving you an unfair advantage.

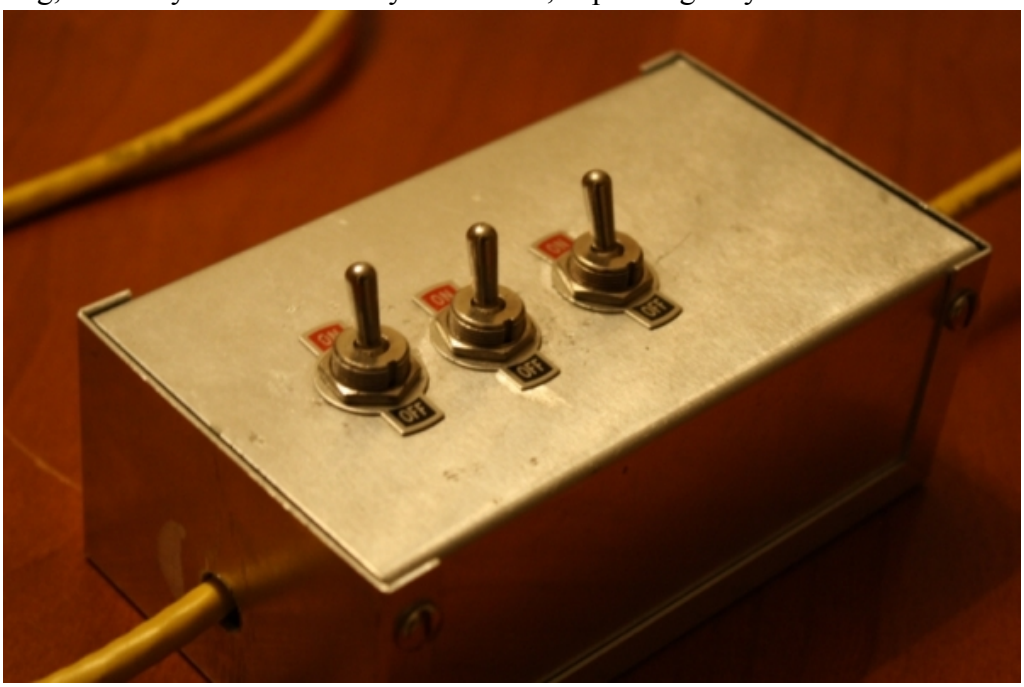
You must use a lag switch with discretion – in an active fight, you'll appear to freeze and will still be vulnerable to attack (note: lagged out players are susceptible to melee attacks, but not bullets). Because you've cut your connection to the game, you also won't be able to see other players moving, so a fair bit of guesswork will go into predicting their actions while you're Frodo'ing the fuck out in the Eighth Dimension. If you use it correctly though, you can effectively ambush other players (for example, some noob picking flowers who is not expecting you to suddenly appear). It's also useful for fighting opponents who are waiting for you to make a move. If somebody is taking cover at the end of a corridor, daring you to make a suicidal charge towards their hail of bullets, you can just drop out for a second and appear behind them, totally catching them off guard. Then you just fuck up their face with a brick until they call you “mommy”. As long as you don't use this tactic *too* often, and avoid being seen by admins, you probably won't get caught. If people make lag-switch accusations, just pretend to lag randomly and act confused. They can't prove anything unless you get cocky and show off your wizard-powers.

Lag-switching can sometimes also be used to gain access to restricted areas. Objects in the world which use a non-tileset graphic (.gif or .png images) often serve as barriers because their scripts designate them as solid objects. Your game client will cache the level in an offline file, but it won't cache those scripted objects and their positions. Go to a room with a barrier (let's say an image of a fence), and then go to a room directly outside of that room. Type in /reconnect to reconnect to Era. This will purge your client's memory of the target room, but a cached version, containing only tiles, will remain. Engage your lag switch, enter the target room, and you'll notice that the barrier (and all other graphics) are gone. Hurry! Run over to the other side of where that fence is supposed to be, and release

the lag switch. Hopefully, you'll reconnect – on the other side of the fence. You can gain access to PyroTech's inside / employee-only levels like this. I've used this trick to get into old gang bases, admin areas, and closed-off Southridge sections. You can even sneak past Staff Blocks with this trick. It's not fool-proof, but it works well enough. You can also do this to avoid door-lamers. If you know somebody is door-laming outside, just lag-switch behind where you expect them to be and open fire. It'll hurt.

A useful application for lag switches is to circumvent ban notices for several seconds at a time. My account was banned due to my flawless douchebaggery, and I soon found that the “Your account has been banned for 30 days.” window could be avoided by logging in to Era, and engaging the lag switch *right before* you enter the game. The timing takes a few tries to get figured out, but once you've got it down, you can travel for short distances in the world before being disconnected. Using this tactic, I was able to move my banned account from the unstick me point, to the hospital, to the apartments, to the sewers. This allowed me to enter my apartment and ensure that some of my stuff was still there.

I recently built a somewhat more sophisticated lag switch, designed to create different types of lag. “Different types of lag?! Bullshit!” you surely just proclaimed, spraying Mountain Dew across your monitor. My theory is that severing different wires can interrupt the game in different ways, as there are eight wires in a CAT5 cable. Some are used for upstream data, and some are used for downstream data. It would be interesting to create a circumstance where you can see your opponents moving (as you are receiving downstream data), but they cannot see you moving (as you have temporarily suspended your upstream data). I don't know how Graal's networking protocols handle this sort of situation, or if it keeps packets in sync on a millisecond basis. I did a bit of research, and found that only four of the eight wires in a CAT5 cable are actually used, anyhow. I put together this lag-switch, using an aluminum project box and some toggle switches. This sort of thing requires drilling and soldering, so it may be difficult for you to make, depending on your skills and access to tools.



It can toggle three of the four active wires (only three so far, because I need to go buy or scavenge a fourth toggle-switch...). I have found that this can create lag which handles differently, but I have no quantitative information regarding that. Using switch #3, I was able to access some areas which I was unable to access using only a standard lag-switch. A lag-switch like this would likely not be very useful for PVP, but might be handy for exploiting the game and gaining access to certain

places.

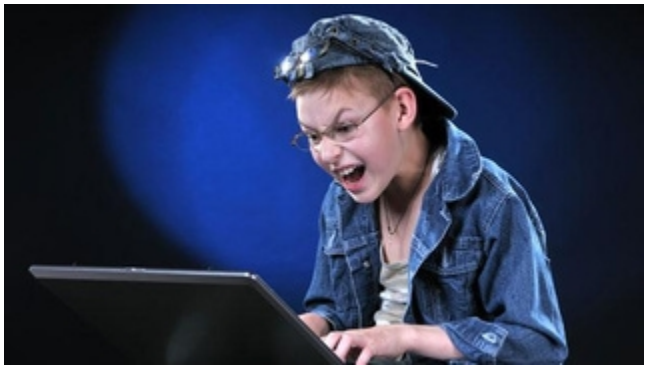
This is purely conceptual, but I think it might be possible to use a micro-controller (such as a cheap-ass MSP430 / Texas Instruments Launchpad) to “pulse” interference through a CAT5 cable. This might create static, so to speak, instead of completely interrupting your connection. It might slow your character down enough to make a difference in a fight. In my experience, potentiometers / variable resistors don't work, because there's still an electrical signal present. Rapid on/off pulses might create better results. I'm no electrical engineer, but if you can build one of these, go for it.

There are apparently software lag switches on the internet, but I imagine those programs can be blacklisted (and subsequently detected) by games and may result in a banning. Hardware lag switches are much harder to detect - as I told a friend "...because you're fucking with the wires, man".

For full build instructions for a basic lag switch, including photographs, consult this guide posted by somebody else online: [http://www.instructables.com/id/The-Lag-Switch/] . I just feel a need to say it – mine are better.

Laming

I think this section is going to be my favorite. Laming isn't strictly illegal, but other players will *totally hate you* for it, which I think is my goal anyway. To those who don't know, laming is the act of using underhanded and deceitful tactics in order to gain the upper hand in a fight. Laming is almost a parallel to what is known as *asymmetrical warfare*, which is what the Viet Cong used to remain effective against better-trained, better-equipped American forces. Instead of meeting a stronger enemy head-to-head in an open field, make him come looking for you in your jungle. Set traps. Appear where you're not expected. Confuse and infuriate him. By the time he gets close enough for a real fight, he's been badly weakened and you'll have the upper hand. I usually lame, because that's just another weapon. My goal is to win, not to have some honorable samurai showdown. The following techniques are infinitely useful at helping you achieve victory.



“This will almost certainly result in unlimited pussy!”

Running – Don't stand around in a fight. Make the enemy chase you. This makes it harder for them because they have to follow your lead while simultaneously pausing to shoot. Use this to your advantage by letting them run into your bullets, or escape if you have to. Lead them down long, narrow gaps and hallways, then turn around and strafe backwards, shooting at them. Or trick them by running in sudden loops or circles around them, instead of a straight line. Moving unexpectedly will break their mojo, because most players aren't used to fighting this way. All the while, make sure to use tons of taunting smiley faces (ctrl+S). This sort of thing typically pisses people off, making them want to chase you even more. You can then lead them through doorways, which lends itself well to

Door laming! - If you know where your enemy is about to show up, stand outside of a door and

swing your ax infinitely (as discussed in the next section). If you have time, place explosives, caltrops, bear traps, or whatever other tricks you may happen to have up your sleeve. If you need to protect yourself from a door lamer (as in, you know that that bastard is out there waiting for you, man. It's a trap!), use a lag switch, as mentioned above. Pop out behind where you expect him to be, and open fire a moment before you reconnect. If you *don't* have a lag switch, wait a few more seconds (this will throw off the other guy's timing), and then run out of the door, holding two arrow keys so you go diagonally immediately. Depending on what type of trap they've laid for you, you have a decent chance of getting past it unharmed.

Sewer Laming – The sewers are my favorite place to lame. Memories, man. If you get somebody to chase you down into the sewers, shoot at the explosive barrels sitting around as they follow you. Grenades, flak and SD cannons are useful down here to go over walls. Make sure you're leading and they're following, and you can abuse the narrow corridors to unleash an unavoidable hail of bullets on them right before you duck and cover around a corner. The sewers are also quite defensible if you have a trio of teamed-up noobs trying to take you down (this is my absolute favorite scenario). Use the sewer's graphics to your advantage: those overhanging sewage channels which you walk underneath are great places to hide traps, making them totally invisible. You can easily knock off a quarter of somebody's health, and make them bleed, with a clever combination of explosives and caltrops. Once you do this, they become your bitch.

Ambush Laming – Walk up to some poor schmoe who is picking flowers, fishing, digging shells, or talking to somebody. Act totally uninterested in them. Take out a trash pick and pretend to be gathering garbage. With this technique, it helps to be disguised as a noob (particularly a female noob), so as to appear totally harmless. Walk slowly past them, and then strike without warning. Even worse, walk up without a weapon equipped and say hello. Ask them a question, and appear to be friendly. As they're typing (which should be obvious, if they pause) run up and attack. You'll hurt their feelings at the very least. With these sort of attacks, you want to open with an overwhelming force – consider using explosive weapons, a Neo Rifle, or a fast series of melee attacks.

You can even “blitzkrieg” a group of enemies by approaching on a Witch Broom or Magic Carpet and suddenly throwing a grenade with G. A note about brooms – if you keep them recharged (charge them while healing in the hospital), you can use Witch Brooms as a sort of rapid assault vehicle. With that kind of speed, you can return to a group of foes who previously killed you before they've prepared themselves for Round Two. They won't be expecting you so quickly, and you'll catch them while they're still healing.

Combat Assistant Scripts

This method is debatable in its illegality, but it certainly provides an unfair advantage. I use it every time I play, of course. I made a script in GlovePIE to automate certain tasks, not because they're tedious, but because it's quicker to make my machine “autopilot” certain input while I'm engaged in combat with another player (or twelve terrified noobs). A good example is band-aid usage. You're down to 19 HP, some douche is shooting at you, and you're bleeding out. If you take your hands off the arrow keys to grab your mouse, open your inventory, and equip the bandages, he's probably going to kill you before you can heal. Unless, of course, you say “Use band-aid!” into your microphone.

```
if said ("Use band aid",6)&& var.graalscriptpaused = 0 {
press(Q)
wait 70ms
press Mouse.WheelUp
wait 40ms
```

```
press Mouse.WheelUp
wait 10ms

mouse.cursorposx = 785
mouse.cursorposy = 476
press(mouse.LeftButton)
wait 70ms
release(mouse.leftbutton)
press(mouse.LeftButton)
wait 70ms
release(mouse.leftbutton)
release(Q)
press(D)
wait 70ms
release(D)
mouse.cursorposx = 1680
mouse.cursorposy = 1000
}
```

Without giving you a full tutorial on GlovePIE scripting (that can be found here: http://www.glovepie.org/w/index.php?title=Preliminary_Documentation_v0.43), I'll go over this fairly simple script. If you say “Use band aid” into a microphone, and the variable “var.graalscriptpaused” is equal to zero (and it will be. I added that variable check to enable me to turn off voice commands if I need to. In your case, the default value is 0, so you're good to go), the script will carry out a series of functions. First, it will press Q, opening the inventory. Then it will scroll up to the top of the inventory, and put the mouse cursor at the coordinates 785,475. Keep that part in mind. It then left-clicks twice, releases Q, presses D to use the band-aid, and returns the mouse cursor to the bottom-right of the screen at 1680,1050. Note that you will have to adjust this script to fit your own needs. If you are running a screen resolution other than 1680x1050, you'll need to set different coordinates. Add

```
debug = mouse.CursorPos
```

to the top or bottom of your script. This will show your mouse's current coordinates in the GlovePIE window when the script is running. So simply hover the mouse over the inventory spot you want to use, write down the coordinates (you might have to switch windows with Alt+Tab to keep the mouse in place), and input them into the script. Change the voice command to whatever you want.

You can put a lot of different spins on this, like doubling the amount of weapon hotkeys available. Using

```
if doubleclicked (z) { }
```

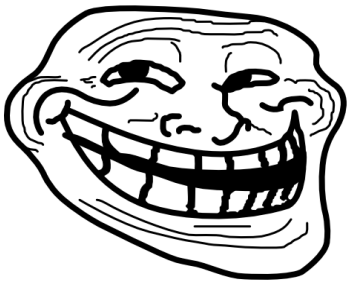
as your key input would run a chunk of code if you press Z twice in rapid succession. Apply this to X, C, Left Shift, Left Ctrl, and anything else you need. You can have unlimited hotkeys, even for weapons which *can't be hotkeyed normally.* Sexy, isn't it?

Here's a really nefarious snippet of code – a melee attack auto-fire. You read that right. Check it out:

```
//Melee Weapon Autofire Begin
If (s) or var.autofiretoggle = 1 //checking to see if the 1 button is "true" (tapped or pressed)
//If var.AF //checking the "on" or "off" status of this variable we affected in the previous statement
s = True //keyboard key s is held
Wait 30ms //waiting 0.1 seconds before processing the next line
s = False //keyboard key s is released
Wait 30ms //waiting 0.1 seconds before processing the next line
EndIf //end the nested statement
EndIf //end the statement
//Melee Weapon Autofire End
```

That makes it so that if you hold down S, you continually press S. This will spam your melee attack. If you have a decent melee weapon, like a Fireman Axe or a Syringe (just something that doesn't break), you can spam your melee attack infinitely outside of a door. To door lame, you just need to hold down the S key now, instead of jamming it for two minutes. Enjoy, you cheating piece of shit. (I mean that in a good way....)

Taunts and Random Chat



You can automate taunts, too. Farting example:

```
 if said ("slash fart") {
  press(Tab)
wait 40ms
release(Tab)
wait 10ms
Type("/fart")
wait 10ms
press(Enter)
wait 10ms
release(enter)
wait 10ms
press(Tab)
wait 40ms
release(Tab)

}
```

You can replace “/fart” with “FUCK YOU”, “plz giv monies I noob”, or whatever else you may want to say quickly and often. I have a *huge* randomized list of insults and taunts, which I can utter based on category. For example, if I say “insult” into my microphone, there's a chance I'll say "You have had sex between zero and two times.". Then again, I *might* say "You're dumber than a boot full of rat cum.". I achieve this by declaring a variable to equal a random number between 0 and 50, for example. Then I make the script roll the dice, so to speak, every two seconds.

```
//Start Random Insult Strings
if var.null = var.null {
var.randomtext = randomrange(1,50)
wait 2000ms
```

```
}
//End Random Insults Strings
```

Then I write out a list like this:

```
 if var.randomtext = 0 {
var.insult = ("You smell like wolf vagina.")
}

 if var.randomtext = 1 {
var.insult = ("Your asshole is square.")
}
 if var.randomtext = 2 {
var.insult = ("Your dick is the wrong shape.")
}
```

Oh yeah, I actually DO have fifty of those. It's horrid, I know. And then, at the bottom of my list, I do this:

```
if said("insult",6)&& var.graalscriptpaused = 0  {
wait 50ms
press(Tab)
wait 75ms
release(Tab)
wait 10ms
Type (var.insult)
press(Enter)
release(enter)
press(Tab)
wait 50ms
release(Tab)
}
```

Which outputs var.insult as my chat text. I also have a category called “Crazy Talk”, where instead of explicitly *insulting* another person, I simply aim to say something whackadoo-insane. Which might also be insulting. Stuff like "EVER FIND A PILE OF SOGGY PORNO IN THE WOODS?! I HAVE! TWICE!", or "I once dicked a man to death with his own dick.". Basically, just frantic, aggressive sexual stuff with occasional drug references. I also have a category for mocking the dead: "*Spits on your twitching body*", and “noob talk”, which is designed to disguise me as a harmless noob and make unsuspecting players lower their guard: "u teach me how to go fishing plz?".

All together, that gives me around 150 random things that I can say at any given moment. It's like if a Furby did cocaine and got really mean. The entirety of this script is included, in Glovepie Script.txt .

Disguises, Deception, And Dirty Fucking Lies

This pairs well with the laming tactics discussed in this document. In order to disarm your opponent before you even initiate a fight, it helps to be disguised. Sure, you've got your normal Graal persona, complete with your favorite color and a head that makes you look cool / tough / like a douche. Leave that look behind for a little while, though. Make sure you get the style saver, so you can keep a veritable wardrobe of different disguises to fit any situation. Of course, experienced players know to

look at your account name, but a simple change of appearance and nickname will fool most noobs, and buy you a few seconds of plausibility when approaching even skilled players. I find that a few categories of disguises work well.

Dumbass Noob – The default "mohawk" look. Pair that with the nickname "unknown" or "billy" or something shitty like that, and you'll look like the lowest of Era's creatures. If people buy this disguise, they'll assume that you pose no threat. Then you strike hard and fast, possibly with a lag switch or Neo Rifle.

Female Noob – Use head6.png with the default noob body. There is some creepy psychology behind this disguise. Most male players will perceive most female players to be less of a threat, as they unfairly judge them to be less skilled and inherently friendlier. There's also a weird "Me am big STRAWNGMAN me show pretty lady me STRAWNGMAN by hunting lady then she know ME AM STRAWNGMAN and give me titties" thing going on in many players' heads, as evidenced by their actions. Use their creepy sexism to your advantage and attack when they least expect it. This disguise is good for getting people to chase you.

Female Non-Noob – A female character with a decent-looking head, like era_head-amy.png or something. Use a lot of red, and an aggressive looking shield, like a katana or something. Instead of chasing you, people will fucking *freeze in place* if you walk up to them and say "Hi <3", because they honestly think that Graal is a plausible method of acquiring random sexual encounters. Like I said, it's weird, but so goddamn effective.

Randomized Disguises – Using similar scripts to the random insults chunk addressed above, you can create a randomized character look with a single voice command. This is great for throwing off somebody chasing you, or for approaching a hostile player who is expecting you, not somebody totally different looking.

Deception is not based solely on looks. On one occasion, there was a player who I deeply despised and accepted a bounty on. He was hiding in a mine, where I would be unable to kill him. I put on the "Female-Non-Noob" disguise and messaged him, striking up a foul conversation which aroused something other than his suspicions. I basically implied that I had some sort of vagina-related surprise waiting for him outside the mine, and he took the bait like a complete idiot. Of course, it was a pile of explosives followed by a hail of gunfire. I killed him within seconds and pretty much shrieked laughter in his face. The lesson here is that you should just say whatever you have to in order to deceive your enemies, and worry about them thinking you're legit-gay after the fact.

There are numerous other hooks which you can use to get people to chase you into traps. You can go to a crowded area (unstick) and yell over and over again "FIRST PERSON TO KILL ME GETS $5000!!", and run around excitedly. Entice people, shoot your gun, use emoticons. Of course, two or three dumb bastards will chase you down and fall into whatever trap you have in mind. You can also bait them by claiming that you're quitting and you're giving away all of your stuff. Psyche people out by pretending to drop guns (be careful not to accidentally drop them for real), and lead your entourage of leeches towards certain death.

You may sometimes have to lie to admins once they catch on to your bullshit and mischief. If other players report you to an admin for something stupid / incriminating / drunk and racist that you said via a private message, you can do something about it. All of your private messages are stored in your Graal/pms folder. Open it up and find the account name of the player whom you minced words with. Open up that text file, and edit it to reflect *your* side of the story. Add a part (with a plausible time-stamp) where the other party called you a faggot. Maybe remove or water down your language. Save the text file, and in Graal in your PM window, click on History and take a screenshot. Boom, forged correspondence. It is worth noting that admins *may* have access to server-side PM logs, but I'm

not sure about that. In any case, show the screenshot to whatever admin you need to in order to argue your case.

I once did this to an extreme degree, in anticipation of future hacking accusations (read more about it below, in *Case Files #1*). I had used my lag switch to access an otherwise sealed-off area. An enemy of mine and his minion saw me in there, and threatened to report me for hacking. I called him a clownfucker and laughed, and got to work. First, I took a screenshot of my profile, showing the "current level" section which clearly showed me on a level where I shouldn't be. I cropped this window and then photoshopped the image – *very poorly.* I typed in the level name over the box in a blatantly shitty font, misaligned, and the wrong color. This image was designed to look fake. I then forged the chat history to paint a picture of my enemy trying to blackmail me with a picture (which I anonymously uploaded online and included a link to), whereby I pointed out how obviously fake it was, and he called me a faggot. I screenshotted this fake message exchange, carefully cropping out the Photoshop bar at the bottom of my screen. With these two screenshots, I'd ensured not only my own safety, but his jailing if he attempted anything. If you want to get an enemy of yours jailed, you can also instigate another player (whom you judge to be too stupid to take screenshots) into cursing your name and "harassing" you. Take a screenshot and bitch to an admin about it once your enemy finally says something hostile. Play the part of the sad innocent kid.

When lying to admins, go big or go home. Hit them with something totally batshit crazy, and at the very least you might confuse them enough so as to throw a smokescreen of doubt over whatever you did wrong.

Client Modification

Graal's client is extremely easy to poke at. The game has a standard tileset and other media assets, but the vast majority of content is downloaded to the client as you play. For example, if you go somewhere in-game with a car or a sign or something, the client will download a .png or .gif file of that sprite. After roaming the world for an hour, you'll have thousands of small image files tucked away in subdirectories in your client. Many of these sprites are designated as "solid" by the game, meaning that a player cannot walk through them, preventing access to certain areas or otherwise impeding the player. With a simple image-editing program (MS Paint), you can resize the image to 1x1 pixels, and reload the client. Ta-da, you now have a solid object which is only one pixel, and can thus be easily avoided.

This is a well-known trick, however, and the developers have created a system to check for tampering. If client-side mischief is detected, you're disconnected. I discovered that (in Windows, at least), setting the modified file's access permissions to "Deny" will prevent the client from snitching on you to the server, and you'll be free to remove anything you don't like. In the past, I've removed barriers, much like in the lag-switch examples above. I also used this method to disable trees in the game, which made it much easier to search for litter while trash picking, because there were fewer visual obstructions.

I've also modified certain image files to make it easier for image-recognition bots to function. For example, I'll make one pixel purple, and then my bot will know what to click on. I also made a variant of the game's tileset containing only solid black and white tiles, indicating solid and non-solid. My intent with this was to make pathfinding easier for an ill-fated trash picking bot (maybe I'll get it to work some day....). Sometimes the easiest option is to just change how the game looks.

Extra Accounts

Obviously you want to avoid doing nefarious bullshit on your main account. That's where you keep your guns, man! Running bots and scamming is best done on throw-away trial accounts. You can easily make as many as you want on the Graal website. For email addresses, just use the “Ten Minute Mail” service (Google it), which gives you a random disposable email account for ten minutes. Make your account, save the login credentials in a text file, and get right to it. Extra accounts are good for farming the “Daily Freebies” which Era is currently giving away. It might be tedious, but it you logged on to a dozen different accounts once per day, you could rack up a huge stockpile of valuable consumable items fairly quickly.

You can also use these accounts as your secret offshore bank account in Switzerland and/or the Cayman Isles. Drop your ill-gotten cash or items in a secret, low-traffic area (in the sewers or in the bank's upper floor or something), pick them up there, and store them on your bitch account until the heat dies down.

It is worth noting that your IP address will be logged and associated with accounts. I recently went around trying to give “something useful” to a user who owned a business (Shrimps, you rich bastard...). My goal was to sell a stocking bot to him, but I didn't specify that. Instead, I gave him a link to an online chatroom to go to if he was interested (so as not to leave records on Graal). He snitched on me to an admin, who warped me to jail and told me the name of my main account. He asked what that useful thing was, and I told him it was information about safe sex. That lead to a speech about spermicide. He warned me, which is fine because he had nothing to indicate what that “useful thing” was. Could've been bots, a USD offer for guns, stolen passwords, anything. I left no proof of a crime, though. Do the same with extra accounts.

Covering Your Tracks

Of course, you're going to want to connect anonymously sometimes. There are a few good ways of doing this. You can connect to Graal on a computer at a different address (your friend Pete's house, McDonald's free Wifi, hell, do it at work if you're one of the 3% of Graal players with a job), or you can use VPN software to essentially play via proxy. Hotspot Shield was recommended to me by some random anonymous hacker who attempted to phish my account by pretending to be Stefan. I used Hotspot Shield while attempting to defeat Era's Graal Relay protection. It works well enough for limited use. You may also want to make sure you spoof your computer's MAC address, and of course, use fake accounts.

Farming Mystery Coins and Treasure for ~~Fun and~~ Profit

Mystery Coins are a new addition to South Ridge. They are tokens hidden around the Southern part of the map, which you can put in a sort of slot machine that spits out random items, including rare guns and expensive hats. As of this writing, there are nine coins:

1) South Ridge Flower shop, back room, hidden in one of the plants.
2) Fire Hydrant outside SR parking garage.
3) A floating corpse underneath the Era-Southridge Bridge
4) One of the plants on the dock on South Ridge
5) Trash can inside SR hospital lobby
6) The small crate outside the SR fishing shack
7) One of the dead cops hidden in the wooded area outside the quest, on the East end of SR.
8) The blonde NPC on the roof of the SR shell shop
9) The tree at the southern edge of the map, at era_present_ac-12.nw 54,60.

Of course, you can go grab all of these coins, do a little dance, and roll the slots nine times in that shack in the wooded area (or three times, if you play the high-stakes slots). Maybe you'll get something awesome, but probably not. You'll need more coins. Refer once more to the “Extra Accounts” section above. Go make one, and try to get the coins. You'll see an error message stating that you'll need 1.5 days of playtime (36 hours) to get the coins. This restriction also applies to dropping money and transferring it with an ATM. In order to reap the benefits of your extra accounts, you'll need to idle them for a while first to rack up 36 hours of online time. To do this, you can just use an idling script and leave your computer on all day while you go live your life.

```
if var.run = 0 {
var.run = 1
wait 1seconds
press (left)
wait 100ms
release (left)
wait 10minutes
press (right)
wait 100ms
release (right)
var.run = 0
}
```

I think that Era has disabled the automatic disconnect which used to happen after twenty minutes of no activity (probably to artificially boost the player count), but run the idling script just in case. It just

subtly moves your character every ten minutes. Park him somewhere indoors and low-key, like a post office or something. Once you hit 36 hours, you'll be free to farm those mystery coins, and maybe get something awesome this time around.

You can also dig up buried pirate treasure. How droll. Every day, five “X Marks the Spot”-style buried treasure locations will spawn on the GMAP, either on grass or sand. You need to dig treasure up with a shovel, and you can only dig up one treasure per account per day. Of course, this is where extra accounts come into play yet again. The contents of the chest can include $1000, an ET coin, or a mystery coin. Treasure spawns at midnight server-time (1:00 on America's East Coast). Many X's will spawn out of sight under trees. This can be fixed by modifying Era's tree image file, instructions for which can be found in the above *Client Modification* section. The image in question is C:\Users\[Your dumbass name]\Graal\levels\images\downloads\era01-tree-summer-tarus.png. Go nuts.

Running Multiple Clients

So now you have a few disposable Graal accounts. By default, Graal prevents you from running more than one instance of the client at a time. Luckily for us, whoever programmed this feature was retarded. To avoid detection of a second client, first install a second copy of the Graal client somewhere on your computer. Rename the main directory something else – for example, “bot client”, or “Zelda with guns”. It can't hurt to rename graal.exe as well. Once you've done that, grab a copy of this application: [http://hawflakes.unoc.net/?p=73]. It's a utility which can rename windows. This will prevent Graal from detecting that a second (or fourth) Graal window is open. Launch your first client, connect to Era, and then use Window Hider to rename it to something else. Once this is done, launch your next window. You don't have to rename it, unless you want even more instances open. Just don't have more than one window called “Graal Era” open simultaneously.

[Note: Window Hider won't permanently rename windows. If you exit the client and come back the next day, it will be called “Graal Era” again, so you've got to rename the window every time you launch the client.]

This is useful for a number of reasons. You can run a bot in one window while playing on your main account in another. Or, you could transfer items quickly via item drops without having to worry about somebody finding your sewer-treasure before you can get back to it. If you're ambitious enough, you could even have a large number of bots running in many different windows, earning you tons of money fairly quickly. Having multiple personas simultaneously might even be useful for scamming and/or social-engineering other players, though I've yet to attempt anything like this.

Running Blacklisted Applications

There are plenty of programs out on the internet which will allow you to cheat on a deeper, more technical level. The two prime examples are Cheat Engine [http://cheatengine.org/] and Winsock Packet Editor [http://wpepro.net/] . If you run either of these programs while Graal is running, the client will instantly detect them and warn you with a scary “Cheaters will be banned!” message. If you keep trying, guess what? You'll be banned. Luckily for unscrupulous bastards such as you and I, Graal isn't too great at detecting what's running on your system. As demonstrated in the *“Running Multiple Clients”* section, you can fool Graal pretty easily. Install your cheating tools to a folder with a different name from the default install path. Then rename the executable files to something inconspicuous, like “blah” or “unicorn penis”. Finally, open them *before* your Graal client, use the Window Hider tool to rename their windows, and then launch Graal. This should prevent detection. Easy.

BONUS! If Graal detects a window with a suspicious name, such as “Cheat Engine” or “Graalrelay”, it will disconnect you, *even if that window is an internet browser*. This can be abused to fuck with other players. You can PM your enemy with a link to such a website. This will require you to test a website (or even set up a page of your own somewhere with a window title named after some cheating software) and disguise your link so as to entice them to click on it. You can disconnect people like this.

Using Blacklisted Applications

This one is actually pretty tricky. As in, I haven't done much in this category. I'll just share what I know, and possibly point you in the right direction.

Cheat Engine is a memory-editing program, meaning that it directly alters values in your computer's RAM. Computer memory works by storing numerical values at certain addresses. Every variable in the game has an address and a value. The amount of cash you have (let's say $10) is stored at an address. Arbitrary example:

0003F300 000A

That looks strange, right? The part on the left is the address, and the part on the right is the value. It's in hexadecimal, not decimal like a human being (or even a yeti) would understand. Add to this the fact that there are literally *millions* of constantly-changing variables in a game's memory, and it becomes overwhelming pretty quickly. Cheat Engine has a feature to help you find which values to fuck with, though. There's a logic engine which allows you to search for values, narrowing down your search criteria until you find the right one. Basically, you do a scan of the game's memory. Then, in-game, you change the value you're searching for. For example, you can drop a dollar, thereby decreasing the memory value. Then you open Cheat Engine and do a search, specifying that the value has decreased. Pop into the game, make four dollars, and search for an increased value. Then you can walk to a new area (which will change thousands of unseen variables by loading new data) and do a search where you specify that the value remains unchanged. After a few passes, you should find the right address and be able to set your cash to a long series of nines.

Of course, it's not that easy. Graal (and most modern games) uses something called “memory pointers” to deter cheaters. Essentially, instead of having your cash controlled by one address, it's controlled by a secret address which changes every time you launch the game. This pointer literally points to the address, meaning that even though you change the pointer's value to 9999999999^2, the real cash value is unchanged. This necessitates a search for the real address. That's hard as fuck. Also, Graal stores player inventories in the server's memory, not in the client's memory. So even if it *looks* like you've got millions of dollars, you actually don't. Cash values are difficult to edit, but there are many other less conspicuous variables in the game which you can edit to your benefit.

Winsock Packet Editor is an even more arcane and difficult application to use. It allows you to manipulate the flow of network data from your client to the server. You can essentially make your computer lie to the server and say “Naw dude, I totally just picked up trillions of dollars, it's cool”. I recommend using a program called Wireshark to monitor and capture your network traffic, allowing you to find patterns and analyze what it going on between the client and server. I have even less experience with this method, though. Like I said, it's arcane. You'll need at least a level-four neckbeard to cheat with WPE, and seeing as how I literally just had sex like, 45 minutes ago (with a girl even!) , I'm not neckbeardy enough. Sorry, Google it.

Using Graal Relay

1. Introduction

Graal Relay is a debugging tool created by a guy named Nalin. It has since become the most notorious (or downright mythical) hacking tool for Graal. Essentially, it works by creating a proxy server on your local computer, through which Graal's network traffic must pass and be subject to your scrutiny and tampering. This allows you to download scripts from servers, log packets, change your character's gani, ignore specified scripts, and even inject code into the client.

Graal Relay has not been published online[2]. As a result, very few people know about it, and even fewer have a copy. I had to do a lot of searching to find somebody who would give me a copy (and you'd be quite surprised to know who![3]). Graal's assorted staff and admins seem to fear the relay over other tools, as they rightly should. It is difficult to detect, and in the right hands, hard to stop. As of this writing, a copy of Graal Relay has been in my possession for less than 24 hours. I am still trying to learn how to use it, but of course, I will pass that knowledge on to you.

2. Setting it Up

This is explained in the included readme file, but I'll restate it here for your convenience. To set up the relay, open up your Windows hosts file with a text editor (Notepad works), at C:\Windows\System32\drivers\etc\hosts . Add this line to the bottom of the file:

127.0.0.1 loginserver.graalonline.com

Save your changes. This will enable Graal-related network traffic to be routed through your computer. In order to play Graal normally again, you'll have to remove that line (otherwise you won't be able to connect without routing through Relay).

Make sure that your Graal Relay folder is named something innocent-sounding, along with the executable file inside (I named them both GR, for example), otherwise you'll receive the “Cheaters will be banned!” message and won't be able to login. Once everything is set up, open Relay first. You'll see a simple black command-prompt style window, which issues the warning that Graal Relay is not suitable for hacking, because it can be traced. This may be true, but this tool is so powerful that it is worth the risk. After opening the program, open your Graal client, and log in to a server. As of now, Era has some protections in place which prevent Relay users from logging in. It detects the program (I believe it looks at the hosts file to do so), and spams the client with either network data or graphics rendering calls to crash it. This will require some work to circumvent. I spoke to MoonDeath about Era's relay detection, and he told me that, once first detected, Era adds your IP to a blacklist. Graal Relay comes with a settings.ini file which allows you to block specified scripts from running, and also inject scripts downloaded from other servers. I have included a customized settings.ini file which blocks many hack-detection scripts by including this chunk:

```
[Server: Era]
blocked_weapons = *,-VID,-Commands,-SpamLoop,-CheatDetection,-MoveSystem,-HackDetection,-
```

2 Until now. A copy of Graal Relay is included with this release.

3 Nalin gave it to me. I just asked him for it over AIM, and he wrongly assumed I wasn't going to include it in a massive cheating guide.

```
HackDetection_Freeze,-HackDetection_Images,-HackDetection_Movies,-HackDetection_OnWall,-
SpeedHackDetection,-Trace,-Polling,player_lang,player,systemactions,-System2,-System
inject_weapons = -EnableFeatures,GraalControl
```

3. Command Syntax

Graal Relay includes a text file which lists the available commands. To use these commands, simply enter them into Graal's chat window.

```
SERVERWARP                  /serverwarp
INJECTWEAPON                /inj
INJECTFLAG                  /if
INJECTFLAGCLIENT            /if_client
INJECTTRIGGERACTION         /it
INJECTTRIGGERSERVER         /it_serverside
GANI                        /gani
INJECTWEAPONGS1             /iwgs1
```

The portion on the right are the commands which Relay listens for, but they're only the default name. The commands themselves can have their names changed for your usage. Most Graal servers have protections in place to look for players who say suspicious things like “/gani” or “/inj [script]”. I highly recommend that you change the commands to something different in order to remain stealthy. Most of these commands are difficult to use and require parameters. For example, /gani requires the name of a GANI animation parameter, which will forcibly set your character's animation state to whatever you specify. /serverwarp will warp you to a specified server, and /inj will inject a script in your weapons folder. To get weapons, copy their scripts from weapon_dump/[server ip].[4] Weapons and scripts are downloaded to your Relay folder when they are loaded in-game. While the actual text files are not verbatim copies of the scripts (they are somewhat corrupted due to network compression), you can get a good idea of what a script does by reading through it. Based on this criteria (or simply the script's name), you may want to block it or inject a script from one server to another. For example, if you get access to staff tools on one server which allow you to fly around, you can take that script and inject it into another. I used Era's fast walking system to move quickly on other servers during testing, for example.

Of course, you can also write your own scripts to inject, which is where this gets really interesting. Using the “Ultimate Graal DVD Torrent” (see “Other Attack Vectors” below for a URL), you can get a copy of a dumped Era backup. Most of Era's core scripts, such as money, damage, and mining, have remained the same for years. Using the information in that torrent, you can write custom scripts to take advantage of this fact and do just about whatever you want.

4 Note that this require `dump_weapons = true` in settings.ini

Gani Hacks

Graal uses animation files called .ganis. It stands for “Graal animation”. Probably. I don't fucking know. Anyhow, these Graal-specific files are used to control how player sprites are animated. It basically cuts out frames from a sprite sheet and turns them into animations for walking or grabbing. One particular exploit uses a modified version of grab.gani to teleport the player around. The modified gani contains instructions to plop the player down a certain distance away whenever the grab animation is played. This exploit seems to have originated with the shitty little iPhone version of Graal[5], but it is applicable to the PC. Most servers seem to have detection in place for this exploit, but I imagine that if you used the same approach for (let's say, “shoot.gani” or something) you could achieve similar results. I've tried modded ganis of various types, and Era detects them. As randomly stupid as Graal's security is, however, I'm sure a gap can be found somewhere. Try modifying grab.gani's access permissions like other modified files, that might work.

In-Game Exploits

Era is not coded to high standards. New content is rarely released, and when it is released, it is usually pushed out not by a cohesive team, but by some guy who just wants to release his little script so that the admins will fucking leave him alone because goddamn yous guys how u expect 1 person to posibly complete so much work bby himself an get pissed when it not done fast?! That is literally the whiny little bitch-attitude which precedes the release of every new item, gun, event prize, area, or game system. There is little-to-no quality testing or peer review. As a result, the game is full of esoteric glitches and strange inconsistencies. These problems are rarely fixed, either due to ignorance of their existence, laziness, or a new generation of scripters who simply don't know how the labors of their predecessors function. A few examples:

The Monk Staff – This is a melee item with a “Bamboo Dash” ability. When you press H, you dart forward a few units. The script seems to attempt to use collision detection, and prevent the user from bumping into solid objects. That works *most* of the time, but it lends itself well to exploitation. Certain solid areas can be bypassed with the monk staff, allowing you to jump to the other side of obstacles. There doesn't seem to be much of a technique to it, and I can't figure out why only certain walls are susceptible to this glitch. Many player houses can be breached this way, if you try to access their secondary entrances on porches or rooftops. This allows you to get to certain restricted areas, and maybe new ones in the future. Paired with lag switching, image-editing, and the grab.gani exploit (if you can get it to work), you could get into most areas.

Gang Perks – I recently discovered that you can maintain gang perks by unlocking them and then quitting your gang. To those who may not know, gang perks are special powers given to you for capturing enemy gang bases, such as the ability to leech HP from opponents with melee attacks (at +12HP per hit with a fireman ax, you can door lame exceptionally well, and even come back from the dead), revive dead players, have a random chance for a critical hit, and make more money from killing gang members. The Blazian Bandits Leech ability has been the most useful for me by far. In a heated fight, you can quickly heal yourself with a cheap melee shot. If you hole up somewhere and door-lame with a riot shield, the combination of leech healing and the shield's defenses will allow you to hold almost any location against multiple attackers. This is excellent for getting quick, easy, hilarious kills if

5 Posted by some middle-schooler here: http://xgraalonlineclassicx.blogspot.com/p/graal-admin-warp-hack_21.html
The file itself is included with this release.

you agitate some noobs.

There are other abilities (usually five or six in total), but gangs seem to change every few weeks, so the information may well be outdated by the time you read it. In any case, get into a gang (any gang. Prestige is not your objective, just join one), wait until night when nobody is online, and capture every single base. Once you've gotten every available perk, quit your gang. Just like that, you've got super-powers that no ordinary player is supposed to have. I have no idea how long this glitch will last, but it was undoubtedly created by some numbskull admin who never checked for glitches. In any case, my perks remain permanent (for now). Enjoy yet another unfair combat advantage (they're just piling up by now, aren't they?)

Gas Canisters – These are event items, but recently have been given away as the "daily freebie". You can drop poisonous gas grenades on the ground which can kill players. I once saw an interesting exploit which a player used to spawn tons of items. She had two or three bitch-noobs working for her who walked into the gas clouds and died from the fumes. Then they died over and over and over again in the course of a few seconds, dropping tons of killdrop items. She was farming for ECs and Golden Coins. I happened to grab ridiculous amounts of other items, like pizza and tacos. It was a good day. An admin soon showed up and watched for a moment before banning her. I played stupid, and he warned us (us being some noob that was in attendance) to forget about what we'd seen there that day. Fuck that. A day later, I attempted the same exploit on a dummy account. I couldn't get it to work, and a different admin showed up to hover over me. I played dumb again, and he left. I don't know if this exploit was fixed or if I'm missing a step, but the concept remains useful. Era's death system is quite fragile, and I'm sure there are other ways to abuse it for items.

Account Theft

Here we go, this is the spooky part. Strictly for legal purposes, I (an anonymous entity whose name is in no way associated with this document) *do not advise, under any circumstance, that you attempt these techniques. I would also like to state that this is purely hypothetical, as I have tested these systems but I have not used them to compromise anybody's account or personal information.*

Graal stores passwords in your computer's registry. On a Windows machine, you can access your registry by going to Start > Run > and typing in "regedit". This will open up a program of immense dark power, a Lovecraftian menace whose core pulses with danger and fury. In other words, don't fuck around here if you don't know what you're doing. All sorts of program-specific data is stored here. Navigate through the folder hierarchy to reach HKEY_CURRENT_USER\Software\Graal\Client . You'll find registry keys containing your login information – on the left, your account name, on the right, your password. It is in an encrypted format, which I initially tried to crack. I have no idea what type of encryption Graal uses to store passwords, but it doesn't matter in any case. It's possible to simply steal the encrypted password hash and manually paste it into your registry in order to access another account. Of course, to do so you must first steal that password hash. This will take you on a (hypothetically) dark journey through a Rube Goldberg machine of deception and technical jankiness. My prototype system worked like this:

1) I find a target. Use a shit-account and a disguise, as described above. Entice him by pretending to be a pretty pretty lady. Offer to send pictures of your tits, and make his life complete.
2) Assuming he agreed with great enthusiasm, send him a .rar (or .zip, if you're a failure) to his email address from your (obviously fake, proxy-accessible) address. There will be two files inside of this .rar file. One is called pic1.jpg. The other is called pic2.jpg.exe. Can you spot the

difference between these two? One is a picture of some random girl's cans that you found on Google Images, and the other is an executable file disguised as an alternate angle of those cans.

3) Once the mark opens the executable, a few things happen. It runs code which it downloads from a free website of yours, becoming a visual basic file and a batch file.

4) The files quickly copy the Graal section of the registry (and *only* that section. You want to leave the rest of their stuff alone, and you don't want to bog down your attack with useless data), and write them to a .png file with a random five-character name. This part is important to make the next step work.

5) The batch file opens a connection to an FTP server which you also set up. It uploads your .png file. Here's the genius of that: most free FTP services only allow certain file types, partially to prevent this sort of bullshit from happening. The .png file is just a text document disguised as an image. It won't load in any image viewer, which is fine. It will hide the fact that you have stolen registry data just sitting on the internet.

6) Once the .png file successfully uploads, the batch file deletes itself, the visual basic file, the .png file, and pic2.jpg.exe., in order to hide what has just happened.

7) You open your FTP browser, fetch the file, and open it in Notepad. Copy, paste, play, prison.

In testing, this whole process typically took about two seconds, from the time the executable was opened to the time the registry file was uploaded and the evidence deleted. Any user stupid enough to open your files will probably miss it entirely, and hopefully have no idea what has just occurred.

If you want to attempt something really ballsy, somehow bait an admin or other staff member (such as an LAT) into falling for this trap. Learn his or her sleep schedule, and once they've logged off for the night, log in using their stolen password hash (RC passwords can be stolen in the same way, they're just listed under a different registry key). Find a level to edit, and discreetly add a script which will give a player $100,000 if they say a certain message (such as a 32-character random string of letters and numbers which nobody else will ever say in this area.). If you manage to make this work, test it once on a disposable account, and never log in to that admin's account again. Wait a few weeks before spawning tons of money.

Unlike with my other techniques, I'm going to withhold the source code and files for this one. I've laid out the basic plan. If you have the skills to do this yourself, then I can't stop you or be held responsible for your actions. At this time, however, I don't wish to distribute this tool and be directly responsible for your dumbass actions.

You can also be a lot less discreet about it and set up a phishing site online. Find some free webhost and create graallogin.bonerpillspamhost.biz, do your best to make it look legitimate, and pretend to be Stefan sending out beta invites to try Graal 2 (“You'll need to login to download the client, of course.”). This approach was actually aimed at me yesterday. I initially saw a PM from “Stefan” and thought to myself “This is it. He knows what I've done. Global ban imminent”. It was just some phisher, of course. I asked him if he was using anything to hide his identity, and he referred me to a tool which I address in this document.

Other Attack Vectors

Here is some hypothetical shit which might work well if you approach it the right way. This is the sort of stuff that I think about when I'm taking a shit, but haven't really attempted myself. It's all loose, conjectural stuff which might be worth exploring if you've got the skills to do so. It also might be totally useless. I'm not sure about this stuff, so here you go.

Super Rewards Exploitation – You can buy Gelats (Graal's shitty pretend currency) for real-life mommy and daddy monies. You can then convert it to in-game items like Lightweight / Worker's Potions, or Graal subscriptions. Gelats can also be earned by trudging the wastelands of their Super Rewards site. Basically, that is where you pull your asscheeks apart and allow spam and advertisements to pour right into your lower torso and occupy your husk like some horrible South-American waterborne parasite. You can sign up for a Netflix trial, or take surveys, or that sort of garbage. This creates a loose patchwork of various corporate ad-sites and personal information forms. I think it might be possible to find a weak website on their list of "partners", and do some good old fashioned browser hacking. By modifying your cookies, or spamming and editing requests with a tool like Fiddler2, you might be able to rack up thousands of illicit Gelats which you can then convert into winning at Graal. Just use proxies, because if you fuck with Graal's bread n' butta like that, they are going to be *pisssssed*.

You can also buy Gelats by texting a certain number, or using one of several other payment options. I'm sure at least one of these payment options has some sort of esoteric trick or exploit which you can abuse for free Gelats.

Exploiting Era's Scripts – Do a Google search for "The Ultimate Graal DVD", (or just go here: http://forums.graal.in/forums/showthread.php?483-Ultimate-Graal-DVD-%282gb-of-Graal-Files!%29-**-Updated-Now-200mb-Rapidshare-Links!-**). It's a torrent download containing *tons* of archived Graal stuff, including leaked server dumps. There's an old version of Era in there. I'd bet that there's some script in one of those files which still exists in modern-day-Era, which can be exploited somehow. Having access to all of those scripts might enable you to find something. It's up to you to figure out how to do that.

Spamming Kills – After two or three kills in a row, you are generally not credited with kills due to spanking your noob too hard. Kill drop items might still appear, though (I'm not sure). You could conceivably set up two disposable accounts, one of which you'll kill over and over again. You could probably even program a rudimentary navigation bot to make the bitch-account walk out of the South Ridge hospital over and over again, into the door-laming volley of your collector account. Rack up some goodies, hide them in the sewer, and pick them up with your main.

Farming Event Coins – Several times per night, the Events Team / Event Bot hosts Chance (or Explosive Chance). Statistically speaking, it is quite possible to win these events simply by clicking on "JOIN EVENT" and standing still. I once did this legitimately. I joined the event and got some coffee (or hell, maybe it was handjob, I can't remember...), letting my character simply warp and sit there. When I returned fifteen minutes later, he was still dancing with his Event Coin. Using this logic, you could make a bot which does nothing but wait around to click the event button. This would be a really slow and inefficient way of ~~earning~~ gaining coins, but totally plausible.

Case Files

Story time! Here are a few examples of my misdeeds and dickish adventures, carving a path of fire and destruction through Era. You may recognize some elements of these stories from the techniques described above. This is where they came from. My hope is that you will learn from (or at least be amused by) these true anecdotes.

1. Lies and Carnage in an Abandoned Gang Base

There was, at one point, an abandoned gang base (Scelus) slightly East of the hospital. It was only accessible via an underground hallway which lead into a room with a ladder, leading down into a hallway which was blocked by staffblocks. I, being the ever-inquisitive sommabitch that I am, decided to gain entry to the nethers of this cavern by using my lag-switch to get past the staffblocks. This worked quite well, and I was able to enter an elevator which took me to a now-deleted gang base. An enemy of mine (who I later made a psychological profile of, in order to help me plan against him) took notice of the fact that I was in an inaccessible area. He lead a posse of similarly hostile demi-noobs to the hallway, where they stood on the other side of the row of staffblocks. He demanded that I tell him how I had gained access, or he would “have me banned”. Scary scary. I called him a cocksucker, laughed, and shot an SD Cannon volley at him and his cronies before disappearing into the elevator.

He sent me a threatening PM, again utilizing his brilliant “I'll tell on you!” strategy. He even said he had a screenshot of my profile, showing me in this off-limits area. He sent me a link to the screenshot, and I quickly edited my chat logs to tell a totally different story. I made it appear as if he had (very poorly) doctored the screenshot by overlaying incriminating text onto the level field. In fact, I had edited his screenshot to make it look like that, and included chat logs which I had falsified. I held onto this image, and even uploaded it online somewhere, in the event that I would need to whip it out to show to an admin. It never came to that, but I still pushed the boundaries by making ambushes on my enemy and his group of three or four others. Scelus Base's lobby linked out to the main GMAP, but seeing as how the exterior of the base was gone, it basically warped me outside. Using this one-way loop, I herded my enemies into the underground area and down the ladder, popping out seconds later on the platform above them, where I chucked grenades down into their pit. The ladder made a perfect chokepoint, and there was no chance of escape for them (especially after I planted explosives on the ladder). This game of cat and down-syndrome-mouse went on for an hour or so.

Below is a cropped portion of my fabricated screenshot, with sensitive information blacked out. It reads from the bottom-up. Notice that the text in “Level” is the wrong font and color, and trails off to the right. This is intentional, so as to look sloppy. The lesson here is that you should have your lies ready to go before you need them. Even if you get caught, just muddle the facts and confuse everybody so much that nobody except for you knows what really happened. Hell, it worked for Casey Anthony.

Oh, ok, let me just fix it up real quick.
[redacted]
Do you think I'm an idiot? That image is clearly an edit! Look, the font is all fucked up, man!
proof that you're hacking, haha your ass is getting banned :)
[redacted]
What the hell is that?
[redacted]
Player info
In-game stats
Real name:
Level:
era_scelusbase-entra
Age:
0
Online-time:
278 hrs 18 mins 28secs

2. How I Got Banned, And Then Came Back Stronger

I logged in one morning and read Era's news. An admin (Sage_Shadowbane, a stupid motherfucker who is now somehow Co-Manager), had released a GUI system for shops. Instead of clicking “Buy” several times on an item, you could now type in what quantity you wanted. I immediately knew what this meant. I ran into Ammo Mart and tested my theory, and holy shit, it worked. This new system *did not sanitize its input against negative numbers*. In other words, I bought -100 boxes of AK-47 ammunition, and was given $700. The shop's stock also increased by 100. I was speechless. Giddy, actually. I quickly logged out and logged back in with a disposable account. Now I truly went wild. Within seconds, my noob-account had millions in the bank. I ran down to Southridge and bought the most ridiculous high-end weaponry I could find. I hid some of it in the top floor of the Era Bank, and came back for it later on my main account.

I must have made, and monopolized on, half a dozen new accounts that morning. In my text file listing the names and passwords of my numerous trial accounts, I marked these with a series of dollar signs. My goal was to spread it out and protect my assets (several eggs in several baskets). I was running around like a madman, absolutely destroying people with a 30-minute-old account, and nobody seemed to notice. It was great. I stocked up my main account with upgraded weaponry, and left my old stuff sitting around in my player's house. I had to leave to go attend to something boring in real life (motorcycle battery), but before I did I logged into Skype with a fake account and contacted one of Era's admins. Anonymously, I told him how the exploit worked, and that he should sanitize the input. My goal here was to try and close the hole so that I'd be the only one to profit from it. He said he already knew what had happened, and that they were tipped off by the fact that the ammo stores had an outrageously huge stock. I walked into Ammo Mart using a clean trial account and saw them there – a cluster of admins, gathered like cops after a bank robbery. I giggled and left. Of course they figured out it was me. I knew they would, and I almost wanted them to. I was bored with Era, and wanted to have a reason to release this document.

When I returned perhaps an hour later, my main was banned, and all of my cash, stats and items had been wiped. This applied to all of my treasure-laden trial accounts as well. I contacted that same

admin over Skype, and told him that he should unban me. I was not asking for a favor – I was making threats. I sent him (a rough draft of) this document, and he said that he might restore my account once my 30 Day ban had run its course. I figured that this was agreeable, because he was actually pretty cool about the situation – he said that, even prior to our conversation, he had made a pre-ban backup of my account because I was "cool as fuck". We even discussed Era's current state, and I learned a few things.

I was able to maintain my ownership of my house / apartment (unspecified) somehow. It wasn't touched because houses expire and are auctioned after 30 days of inactivity, meaning that a ban effectively deprives you of your real estate holdings on Era. I was able to login for several seconds at a time with a lag switch, circumventing the ban message for a moment, and thus I was not "inactive". When I returned to Era, though my account was reset, I still had a home full of exotic weaponry which the admins had missed entirely. Some of it was legitimate, but much of it had been gained illicitly by spawning money.

Unfortunately, the admin who had made a backup of my account had since been banned himself, along with the previous Manager. He was no longer around to restore my account. However, I took advantage of the changing of the guard and actually talked my way into regaining the majority of my stuff. I told the new Manager that, in the wake of his predecessor's shameful downfall, I had somehow gotten banned and been promised that my items would be returned. He never even asked *why* I had been banned. It took maybe an hour, but I talked him into giving me a fucking Christmas list of expensive items, one of which wasn't actually in my possession prior to my ban. I thanked him and went on my way.

As a result of this, I am now stronger than ever. Sure, my total HP is less than it used to be, but it will return in time. I'm already halfway there. I essentially took a break from Era for a month and got tons of new weaponry in the process, because Era has no continuity of government, no procedure, no permanent hierarchy. Nobody even remembers how badly I broke the rules, just a few months ago – it's as if Era has no written history. I blatantly cheated and *got rewarded for it*. Simply put, I won.

3. How I Got Banned, But For Real This Time

All good things come to an end, eh? I was running my very successful mining bot when a group of three admins suddenly warped to my location. I quickly stopped the bot (which would have entered into its "BRB" mode within a second anyhow) and did my best to act as human as possible. They warped me to a cute little interrogation room. One PR (Koho) told me to confess and I'd be let off with a warning. I figured I'd go with that option, lay low for a while, and continue botting in a week or two. After I confessed, they banned my account. I logged in a moment later with a throw-away account and confronted them for this, saying that I'd been promised a warning. Really, I knew what was happening. They were checking logs to find out what else I had done, and what my main accounts were. I had come to make my threats and demand to be allowed to "cheat with impunity". As much as I felt I made a good case for myself, the various admins did not seem to take my threats too seriously, so I've made good on them with the release of this document, Era's Black Book. As I told them, I had a metaphorical gun pointed at Era's head.

Conclusion

So, what have we learned? Graal is an incredibly fragile game, which is poorly staffed and chock full of glitches. As long as you're cautious and maintain a low profile, you can fly under the radar and do whatever the fuck you want. If confronted, you can lie to admins by fabricating evidence to fit your story and discredit your enemies. You can make an infinite amount of extra accounts in order to cloud your identity, store your shit, farm freebies, and run bots. These bots can generate tons of money for you, which you can transfer to your main account in order to buy what you need. You can also use a weight-lifting bot to make that main stronger and more capable. Using tools like Combat Assistant scripts and lag switches, you can up your game and give yourself abilities and rapid reactions which other players simply can't match. You'll confuse your enemies by seemingly teleporting past danger and materializing from thin air right behind them. By modifying image files, using your lag switch, and exploiting items like the Monk Staff, you can access areas which you aren't supposed to. By employing disguises and manipulating peoples' emotions, you can trick your enemies into doing what you want and thus destroy them. By hacking the game's memory and by interfering with network traffic, you can conceivably spawn guns and money for yourself. If you're willing to break the law, you can even steal other players' accounts and all of their resources. The above methods will make you more powerful than anybody wants you to be. That's what you're after, right?

~~Credits~~

~~I only compiled these methods. I didn't invent them (okay, maybe some of them), as many of these are ancient techniques that I first learned about via a wayward mass message or forum thread. I don't remember where I heard about them, so I won't bother with credit. I might publish this anonymously (probably) anyhow, so fuck it.~~

You know what? The above “Credits” section was written well before I finished this document. In retrospect, these methods are mostly mine. I came up with a lot of these techniques, then I wrote a guide on them. Hell, I even built hardware specifically for this. I can say proudly that this whole experience has taught me tons about breaking the rules (particularly how to), about programming, about anonymity, and about power structures (mom says no, so go ask dad). This experience has been my own, my journey through playing Era and then burning my bridges in the most beautiful way I could. I'm probably done with Graal forever now. They won't even let me in the gift shop. See you guys, thanks for the easy kills.

-Crazy Tom, The Sewer Bastard